UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/661,448	09/13/2000	Muriel Roger	T2153-906593	7843

181 7590 11/19/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER
KIM, JUNG W

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/661,448	**Applicant(s)** ROGER ET AL.	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 September 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 September 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 8-22 have been examined. Applicant has amended claims 8-21 and added new claim 22 in the amendment filed on September 3, 2004. Claims 1-7 were canceled in a previous amendment.

Response to Amendment

2. The 112, first paragraph rejections to claims 10 and 17 are withdrawn as the amendments to the claims overcome the rejections.

3. The 112, second paragraph rejections to claims 8, 10-13, 15 and 17-20 are withdrawn as the amendments to the claims overcome the rejections.

Response to Arguments

4. Applicant's arguments filed September 3, 2004 have been fully considered but they are not persuasive.

5. In response to applicant's arguments against the references individually (see remarks, page 7, second full paragraph), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). As outlined below, the limitations of independent claims 8 and 15 are covered by Smaha combined with the teachings of Thuraisingham and Schoning: Smaha teaches, inter alia, extracting and analyzing each

record of a log file and generating either an output file or an action of the computer system as a result of the analysis to implement a high performance resolution method for detecting attacks against a system (see Smaha, Figures 2b, 5a, 6a and 6b), Thuraisingham teaches, inter alia, detecting security violations in a secure database wherein data and constraints are modeled into Horn clauses to utilize standard logic constructions and tests (see Thuraisingham, col. 14, lines 30-46), and Schoning teaches, inter alia, expanding formulas into subformulas and generating Horn clauses for each expanded formula to efficiently test for satisfiability (or validity) of a constraint (see Schoning, pages 23-24, especially page 23, last paragraph and page 24, second paragraph and 'efficient test for satisfiability'; pages 29-35, section 1.5, Resolution, especially page 30-31, definition of resolvent and page 32, Exercise 29). For these reasons and those outlined below, the prior art of record cover the limitations of the claimed invention.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 9 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claim 9 recites the limitation "the formulation of the specification". There is insufficient antecedent basis for this limitation in the claim.

9. Claim 16 recites the limitation "the formulation of the specification". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 8-9, 14-16, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smaha et al. U.S. Patent No. 5,557,742 (hereinafter Smaha) in view

of Thuraisingham et al. U.S. Patent No. 5,694,590 (hereinafter Thuraisingham) and Schoning Logic for Computer Scientists (hereinafter Schoning).

13. As per claims 15, 16 and 22, Smaha discloses a computer system comprising storage means and processor for executing programs for implementing a high performance resolution method for detecting attacks against the system wherein the method:

a. receives audit conditions to be detected using non-limiting specification formulas expressing fraudulent entry or attack patterns or abnormal operations to be verified by examining records of a log file of a computer system (see Smaha, Abstract, especially 1st sentence; Figures 1, 2b, 3, 4, and 5a).

14. Smaha is silent on the matter of expanding the formulas into Horn clauses to detect attack conditions. However, the use of Horn clauses to articulate rules in a security framework is well implemented in the art. Thuraisingham discloses a method for detecting security violations in a secure database wherein data and constraints are modeled into Horn clauses to process the security risk of the data and to obtain a conflict resolution (see Thuraisingham, col. 14, lines 30-46). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Thuraisingham to the invention disclosed by Smaha. Motivation to combine enables the invention to utilize the consistency and completeness of Horn clause logic programs to determine the security threat as taught by Thuraisingham. Ibid.

15. In addition, although Thuraisingham does not cover in detail how rules are specified into Horn clauses, means to do so are found in Schoning. Schoning teaches a method for taking literals, representing an atomic formula being either a positive or negative (see Schoning, page 18, definition of literal), defining a set of formulas from a set of literals having CNF form (see Schoning, pages 19-23), then converting the formulas to Horn formulas, resolving and testing for satisfiability (see Schoning, pages 23-24, especially page 23, last paragraph and page 24, 'efficient test for satisfiability'; pages 29-35, section 1.5, Resolution, especially page 30-31, definition of resolvent and page 32, Exercise 29). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Schoning to the invention covered by Smaha. Motivation to combine utilizes standard means for assigning and translating data/constraints to Horn clauses. Ibid. Hence, this method covers the following steps:

b. expands the formulas into subformulas for each record (see Smaha, Figure 2b as modified by Schoning, page 19, Theorem; page 23, formula F, last equation);

c. scans and generates, for each expanded formula, Horn clauses to resolve in order to detect whether or not the formula is valid for each record, the Horn clauses expressing implications resolvent of the subformulas for each record scanned in positive clauses having a positive literal, and in non-positive clauses having at least one negative literal (see Schoning, page 23, definition of Horn formula; pages 29-35, section 1.5, Resolution, especially pages 30-31, definition of resolvent);

d. stores positive clauses in a stack of subformulas; storing, in a table of clauses a representation of the negative clauses and the positive clauses; stores, in a table of counters, a number of negative literals in each negative clause (see Schoning page 35, 'algorithm to decide satisfiability');

e. resolves the table of clauses based on each positive clause, so as to generate either an output file or an action of the computer system (see Smaha, Figure 5a, Reference Nos. 32 and 42 as modified by Schoning, page 35, 'algorithm to decide satisfiability'; pages 117-131, section 3.2, Horn Clause Programs).

16. Finally, the above steps is implemented by means of: an adaptor for translating information from a log file into a language comprehensible to an interpreter (see Smaha, Figure 5a, Reference No. 12 as modified by Schoning, page 3, 'atomic sentences'); an interpreter for receiving a formulation of a specification in a temporal logic in a specification formula in order to expand the formula and fill in the table and the stack of subformulas stored in the memory of the computer system and resulting from the scanning of the computer system's log file (see Smaha, Figure 5a, Reference Nos. 144 and 142; col. 9, lines 56-67 as modified by Schoning, page 4-5, definition for syntax and semantics of propositional logic; page 9, definition of suitable assignment, model, satisfiable, valid; pages 14-23, section 1.2 Equivalence and Normal Forms); and a clause processing algorithm for resolving the Horn clauses to generate an output file or an action (see Smaha, Figure 5a, Reference Nos. 32 and 42 as modified by Schoning,

page 35, 'algorithm to decide satisfiability'; pages 117-131, section 3.2, Horn Clause Programs). The aforementioned cover the limitations of claims 15, 16 and 22.

17. As per claim 21, Smaha covers a computer system as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). Although Smaha does not expressly disclose scanning the log file only once from the beginning to the end, it is notoriously well-known in the art to implement means to reduce the number of runs for a given task to a minimum. The examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to scan the log file completely only once. Motivation to combine eliminates redundant work. The aforementioned cover the limitations of claim 21.

18. As per claims 8-9 and 14, they are method claims corresponding to claims 15-16 and 21 and they do not teach or define above the information claimed in claims 15-16 and 21. Therefore, claims 8-9 and 14 are rejected as being unpatentable over Smaha in view of Thuraisingham and Schoning for the same reasons set forth in the rejections of claims 15-16 and 21.

19. Claims 10-13 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smaha in view of Thuraisingham and Schoning, and further in view of Cormen et al. Introduction to Algorithms (hereinafter Cormen).

20. As per claims 17 and 18, Smaha covers a computer system as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). Smaha does not expressly disclose representing the table in the form of a matrix or a sparse matrix having columns represented by chained lists. However, as taught by Cormen, these means are the two standard ways to represent relationships between data of a set with at least one other data of the set. See Cormen, page 465, 3rd paragraph, first sentence; page 466, Figure 23.1. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Cormen to the invention covered by Smaha, since sparse matrix and matrix formations are the two standard means of representing relations between data of a set. Ibid. The aforementioned cover the limitations of claims 17 and 18.

21. As per claims 19 and 20, Smaha covers a computer system as outlined above in the claim 15 and 16 rejections under 35 U.S.C. 103(a). Smaha does not expressly disclose the use of a hash table in the step of expanding formulas into subformulas. However, in a different section, Cormen teaches the use of hash tables to efficiently devise a one-to-one mapping structure as an alternative to a direct addressing scheme. See Cormen, pages 221-222, section 12.2, 'Hash Tables'. Formulas stored in a hash table rather then a direct addressing scheme to be expanded into subformulas would be more efficient since the universe of formulas would probably be much greater then the actual number of formulas to be expanded. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Cormen to the

invention covered by Smaha. Motivation to combine enables the formulas to be uniquely addressed but stored in manner that is better optimized for a subset of formulas drawn from a large set of possible formulas as taught by Cormen. Ibid. The aforementioned cover the limitations of claims 19 and 20.

22. As per claims 10-13, they are method claims corresponding to claims 17-20 and they do not teach or define above the information claimed in claims 17-20. Therefore, claims 10-13 are rejected as being unpatentable over Smaha in view of Thuraisingham, Schoning, and Cormen for the same reasons set forth in the rejections of claims 17-20.

Conclusion

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephonic Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
November 9, 2004

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100